Security Incident Response Workflow

Preparation:

Improve Detection Capabilities
Improve/Update Documentation
Improve Interdepartmental Communication
Security Training
User Security Awareness Training
Solicit Community Feedback

Detection Sources:

Notification from MSU Department
ServiceNow Incident
User Feedback
External Notification
Auditing
Threat Hunting
Accidental Discovery

Log Correlation/SIEM
- Linux Host Logs
- Windows Host Logs
- Active Directory Events
- Windows Client Logs
- Mac Client Logs
- Networking Logs

Detective and Preventitive Controls
- Endpoint Protection
- Mail Filtering
- File Integrity Management

Vulnerability Management
- Vulnerability Scanning
- Web Application Scanning
- Web Application Firewall